Do you know your privacy risks?

How new technologies, changing business models, and emerging regulations are changing the data-protection landscape

January 2013

At a glance

Threats to data security—both internal and external—are at an all-time high, yet many utilities do not understand how their data is collected, stored, and used.

The smart grid, expanding regulations, and customer demands are presenting complex new challenges to data privacy.

Utilities should develop and implement proactive data-privacy programs to manage evolving risks and regulations across their ecosystems and beyond.

pwc

The world is changing fast for power and utility companies. Smart grid implementations, ever-expanding regulations, and shifting business models to promote cost effectiveness and customer engagement present new and complex challenges. In an era of lower budgets and higher expectations, utility companies are increasingly—and correctly—concerned that their data is at risk. Today's business environment requires a disciplined focus on securing sensitive information and understanding how data is collected, stored, and used.

The escalation of data risks

Power and utility companies are justifiably concerned about data privacy and security. New technology and customer-engagement channels are quickly being introduced, the volume of data collected is snowballing, and data-use practices are rapidly shifting. Outsourced and cloud services continue to underpin cost-reduction efforts, but they also introduce new risk considerations over customer, employee, and sensitive data within the organization. Given an increasingly mobile workforce with 24-hour access to systems and data through laptops, web portals, and smart devices, the risks in today's data landscape are difficult to define, much less control.

External threats are also evolving, and reports of data breaches and cyber security incidents have become a daily event. The US Department of Homeland Security says that power and utility companies reported 198 incidents of suspected cyber threats in 2011, up from only 41 reported incidents the year before.[1] What's more, PwC's annual Global State of Information Security® Survey shows that the number of utilities respondents reporting 10 to 49 security incidents in 2012 jumped 75% over 2011 and 600% over 2010.[2]

These data incidents can be quite costly: A recent survey by the Ponemon Institute put the price in the United States at $194 per compromised record, or an organizational total of $5.5 million per breach.[3]

$5.5M

The average total organizational cost of a data breach in the United States

1 US Department of Homeland Security, ICS-CERT Incident Response Summary.
2 PwC, *The Global State of Information Security® Survey 2013*, September 2012.
3 Ponemon Institute, *2011 Cost of a Data Breach: Global*, March 2012.

Protecting critical assets and ensuring compliance are nothing new to utilities. But game-changing technology initiatives and heightened public awareness of privacy concerns present new challenges. And as data threats multiply, so do compliance requirements. Legislative and regulatory activity related to data protection and privacy is at an all-time high from both federal and state governments, as well as from public utility commissions concerned about the privacy implications of smart meter data. Today's business environment requires a disciplined focus on securing sensitive information and understanding how data is collected, stored, and used.

Unfortunately, many utilities have not yet implemented the privacy and data-protection programs necessary to safeguard data and address these new risks. Without effective privacy programs, utilities face an increased risk of data loss or misuse that can dent their reputation and imperil good relationships with customers, employees, and regulators potentially resulting in investigations, fines, and other regulatory actions.

As these risks coalesce, power and utility companies should consider adoption of an informed and proactive approach to data privacy.

Data privacy in danger

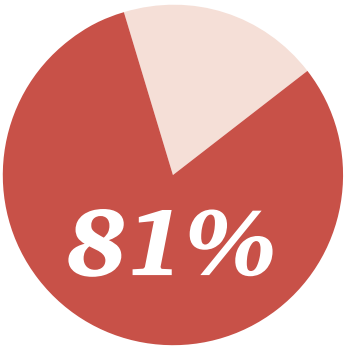
For power and utility companies, new regulations and technologies have combined to make data privacy more important than ever. This is not lost on executives. A global survey of executives and risk-management leaders conducted by PwC found that 62% of respondents rank changes in regulations and government policies as a top risk to their business this year.[4]

Federal legislative proposals over privacy and cyber security are increasingly under debate while state legislatures continue to implement and enhance breach-notification and data-protection laws. Concurrently, utility regulatory commissions are adopting privacy-related dockets with a noteworthy focus on the collection, use, and disclosure of smart-meter data. While many commissions remain in a "fact-finding" mode related to privacy risks and considerations, some states have issued specific decisions. For instance, states have handed down explicit rules regarding the privacy and security of customer energy usage data. Managing these new regulations presents a significant challenge for many utilities, particularly competitive retailers and utilities that operate across multiple states and markets.

While overarching technological advances like the smart grid typically dominate discussions, other factors are also redrawing the privacy landscape. For instance, customer and regulatory demand for improved customer service and access to energy-efficiency programs can challenge traditional safeguards focused on external vulnerabilities. These programs introduce new internal risks based on how customer data is collected and disclosed. A data breach, after all, can originate from insiders such as employees or from outsiders like third-party contractors who receive customer information. Unauthorized disclosure of customer information

4 PwC, *Risk in review*, March 2012.

to a vendor or an e-mail containing sensitive employee data may open the door to damaging events, no matter whether the breach originates inside or outside the business.



Percentage of survey respondents that say privacy is a top 10 risk or initiative this year

Compounding the situation, our security survey found that only 51% of utilities respondents say their organization requires third parties to comply with their privacy policies, and only one-third conduct compliance audits of third parties that handle personal data. Indeed, the very definition of sensitive data, or Personally Identifiable Information (PII), is often inconsistently interpreted across departments and stakeholders.

New technologies and business processes are likely to further impact privacy programs. Advances in web and mobile connectivity, marketing programs that exploit augmented consumer data, and an increasing reliance on third-party service providers may disseminate customer information across increasingly numerous systems, divisions, and business partners.

Utilities may also grapple with challenges in managing the risks and compliance requirements associated with employee data, as well as confidential competitive and regulatory information. That's a challenge for many organizations because they may not know where this data is located or how it moves across the information ecosystem. Case in point: Only 31% of utilities respondents to PwC's information security survey say their organization has an accurate inventory of locations of stored data.[5] Many are even less prepared to control the use and distribution of this information.

Privacy strategy can be further strengthened through comprehensive employee training and awareness. Yet only 34% of utilities respondents to PwC's security survey say their organization has an end-user security awareness program in place.[6] And even when training has been implemented, it often centers on security controls; personnel responsible for handling sensitive data rarely receive formal training on managing privacy risks.

5 PwC, *The Global State of Information Security® Survey 2013*, September 2012.
6 Ibid.

Taking the first steps toward privacy

As the pace of privacy risks and regulations accelerate, one thing is certain: power and utility companies should develop and implement sustainable privacy programs to enable them to proactively manage these challenges.

Key to an effective data-protection and privacy program is engagement with the many—and disparate—stakeholders across the organization who design, implement, and manage the ongoing effectiveness of the initiative. As with most business issues, it is important that support for a data-privacy program begin with top executives and cascade throughout the organization. Support should also come from across the "C suite" to prevent the common misconception that this is only an IT matter.

Stakeholders from departments such as IT, customer operations, human resources, and legal establish the organization's risk appetite for data protection and then drive the implementation of appropriate privacy policies and practices. While existing compliance and risk forums can help govern a data-protection and privacy program, unwavering executive sponsorship and cross-functional commitment to the program's objectives are critical.

Key elements of effective privacy

- Understand your company's compliance and culture
- Align and train management and staff on security practices
- Know your data, where it is, and what must be protected
- Ensure third parties comply with your privacy policies
- Understand your threats and controls
- Test and update controls regularly
- Be prepared to respond to incidents

Equally important is a comprehensive understanding of the data collected, stored, and used across the business environment. Organizations should complete an inventory of sensitive-data locations and understand how that data flows across the enterprise and to third parties. The hard truth is that known data and process flows can be better protected.

To fully determine effective controls for data and processes, organizations should carry out a rigorous risk assessment leveraging their data inventory. An understanding of regulatory compliance requirements is necessary of course but the assessment should also consider threats to the organization's brand, regulatory relationships, and overall risk tolerance. What's more, this holistic risk-based assessment should enable the organization to address a broad range of data-protection and privacy considerations through a single, integrated framework of privacy and security controls. The result? Silos of cross-functional compliance activities will be minimized, and a foundation will be laid for a flexible framework that can adapt to future evolutions in technologies, regulations, and operations.

Control considerations

- Vendor contracting
- Technology security and data loss prevention
- Notice and consent
- Retention and disposal
- New systems and processes
- Use and disclosures
- Data classification

Once risks and the control framework have been identified, it is necessary to assign ownership for the communication and maintenance of controls. Consistent training is essential so that those charged with operating-data protection and privacy controls are prepared to effectively execute their role. While existing information-security training programs can be enhanced to incorporate data-protection considerations, employees with access to sensitive data should receive additional education on privacy policies and procedures. To assess the effectiveness of the overall program, accountability for monitoring should be delegated to management and supplemented with assessments through an independent group such as the compliance office or internal audit.

Utilities can get ahead of this rapidly moving issue and make smart decisions to put in place programs now as new challenges are emerging. Doing so will help prepare for new issues in data privacy—and protect customers and employees from information breaches.

It's time to rethink data privacy

Threats to data privacy are surging. In 2011, more than 500 data breaches involving 30.4 million sensitive records were reported, including some of the largest individual breaches on record.

When these intrusions result in leaks of sensitive data, the damage to a power and utility company's brand, regulatory status, customer relationships, and intellectual property can be significant.

The unique challenges facing utilities compound the need for a holistic, risk-based data protection program—one that addresses the privacy considerations of today yet is flexible enough to manage constantly evolving risks and regulations. It's time to rethink your data-privacy program.

7 The Privacy Rights Clearinghouse, *Data Breaches: A Year in Review 2011*, December 2011.

www.pwc.com/utilities

To have a deeper conversation about how this subject may affect your business, please contact:

Michael A. Herman
Power and utilities assurance leader
PricewaterhouseCoopers
312 298 4462
michael.a.herman@us.pwc.com

Alan Conkle
Power and utilities principal
PricewaterhouseCoopers
312 298 4461
alan.conkle@us.pwc.com

Dave Sands
Power and utilities director
PricewaterhouseCoopers
703 918 3421
david.c.sands@us.pwc.com